CLAIMS

What is claimed is:

1. An apparatus comprising:

a first storage to store a platform identifier unique to a platform;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.

2. The apparatus of claim 1 wherein the signature generator comprises:

a platform-specific transformer to transform the authentication identifier using the platform identifier to output an encrypted platform private key; and

a decryptor coupled to the platform-specific transformer to decrypt the encrypted platform private key to generate the platform private key using an authentication public key, the authentication public key being provided by the authentication vendor.

3. The apparatus of claim 2 wherein the signature generator further comprises:

a signer coupled to the decryptor to sign the data using the platform private key, the platform private key being transparent to the platform.

4. The apparatus of claim 2 wherein the platform-specific transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the platform identifier and the authentication identifier.

5. The apparatus of claim 2 wherein the platform-specific transformer comprises:

a decryptor to decrypt the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

6. The apparatus of claim 2 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key using the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

7. The apparatus of claim 6 wherein the platform-specific reverse transformer comprises an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key using the platform identifier.

8. The apparatus of claim 4 wherein the platform identifier is a unique, serially uncorrelated bit stream.

9. The apparatus of claim 6 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated from the platform identifier.

10. The apparatus of claim 1 wherein the platform identifier is installed in the first storage in a protected environment.

11. The apparatus of claim 10 wherein the protected environment is a system management basic input/output system table.

12. The apparatus of claim 4 wherein the platform-specific transformer further comprises:

a reporting device to report the platform identifier to generate a tracked platform identifier.

13. The apparatus of claim 1 wherein the platform identifier is a processor serial number retrieved from a processor.

14. An apparatus comprising:

an encryptor to encrypt a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

a platform-specific reverse transformer to transform the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform, the authentication identifier being provided to the platform to generate a digital signature.

15. The apparatus of claim 14 wherein the platform-specific reverse transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

16. The apparatus of claim 15 wherein the platform identifier is a unique, serially uncorrelated bit stream.

17. The apparatus of claim 14 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

18. A method comprising:

storing a platform identifier unique to a platform and an authentication identifier in first and second storages, respectively, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

generating a digital signature for data using the platform identifier and the authentication identifier.

19. The method of claim 18 wherein generating digital signature comprises:

transforming the authentication identifier using the platform identifier to output an encrypted platform private key; and

decrypting the encrypted platform private key to generate the platform private key using an authentication public key provided by the authentication vendor.

20. The method of claim 19 wherein generating the digital signature further comprises:

signing the data using the platform private key, the platform private key being transparent to the platform.

21. The method of claim 19 wherein transforming the authentication identifier comprises:

performing an Exclusive OR (XOR) function on the platform identifier and the authentication identifier.

22. The method of claim 19 wherein transforming the authentication identifier comprises:

decrypting the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

23. The method of claim 19 wherein the authentication identifier is generated by transforming the encrypted private key using the platform identifier, the encrypted private key being encrypted from the platform private key using an authentication private key.

24. The method of claim 23 wherein transforming the encrypted private key using the platform identifier comprises performing an XOR function on the encrypted platform private key and the platform identifier.

25. The method of claim 21 wherein the platform identifier is a unique, serially uncorrelated bit stream.

26. The method of claim 23 wherein transforming the encrypted private key comprises encrypting the encrypted private key using a symmetric encryption/decryption key generated from the platform identifier.

27. The method of claim 18 wherein storing the platform identifier comprises installing the platform identifier in a protected environment.

28. The method of claim 27 wherein the protected environment is a system management basic input/output system table.

29. The method of claim 21 wherein transforming the authentication identifier further comprises:

reporting the platform identifier to report a tracked platform identifier.

30. The method of claim 18 wherein the platform identifier is a processor serial number retrieved from a processor.

31. A method comprising:

encrypting a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

transforming the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform.

32. The method claim 31 wherein transforming the encrypted platform private key comprises:

performing an Exclusive OR (XOR) function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

33. The method of claim 32 wherein the platform identifier is a unique, serially uncorrelated bit stream.

34. The method of claim 31 wherein transforming the encrypted platform private key comprises encrypting the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

35. A computer program product comprising:

a machine readable medium having computer program code therein, the computer program product comprising:

computer readable program code for storing a platform identifier unique to a platform and an authentication identifier in first and second storages, respectively, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

computer readable program code for generating a digital signature for data using the platform identifier and the authentication identifier.

36. The computer program product of claim 35 wherein the computer readable program code for generating digital signature comprises:

computer readable program code for transforming the authentication identifier using the platform identifier to output an encrypted platform private key; and

computer readable program code for decrypting the encrypted platform private key to generate the platform private key using an authentication public key provided by the authentication vendor.

37. The computer program product of claim 36 wherein the computer readable program code for generating the digital signature further comprises:

computer readable program code for signing the data using the platform private key, the platform private key being transparent to the platform.

38. The computer program product of claim 36 wherein a computer readable program code for transforming the authentication identifier comprises:

computer readable program code for performing an Exclusive OR (XOR) function on the platform identifier and the authentication identifier.

39. The computer program product of claim 36 wherein a computer readable program code for transforming the authentication identifier comprises:

computer readable program code for decrypting the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

40. The computer program product of claim 36 wherein the authentication identifier is generated by a computer readable program code for transforming the encrypted private key using the platform identifier, the encrypted private key being encrypted from the platform private key using an authentication private key.

41. The computer program product of claim 40 wherein a computer readable program code for transforming the encrypted private key and the platform identifier comprises performing an XOR function on the encrypted platform private key and the platform identifier.

42. The computer program product of claim 38 wherein the platform identifier is a unique, serially uncorrelated bit stream.

43. The computer program product of claim 40 wherein a computer readable program code for transforming the encrypted private key comprises a computer readable program code for encrypting the encrypted private key using a symmetric encryption/decryption key generated from the platform identifier.

44. The computer program product of claim 35 wherein the computer readable program code for storing the platform identifier comprises computer readable program code for installing the platform identifier in a protected environment.

45. The computer program product of claim 44 wherein the protected environment is a system management basic input/output system table.

46. The computer program product of claim 38 wherein a computer readable program code for transforming the authentication identifier further comprises:

computer readable program code for reporting the platform identifier to generate a tracked platform identifier.

47. The computer program product of claim 35 wherein the platform identifier is a processor serial number retrieved from a processor.

48. A computer program product comprising:

a machine readable medium having computer program code therein, the computer program product comprising:

computer readable program code for encrypting a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and

computer readable program code for transforming the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform.

49. The computer program product claim of 48 wherein a computer readable program code for transforming the encrypted platform private key comprises:

computer readable program code for performing an Exclusive OR (XOR) function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

50. The computer program product of claim 49 wherein the platform identifier is a unique, serially uncorrelated bit stream.

51. The computer program product of claim 48 wherein the computer readable program code for transforming the encrypted platform private key comprises computer readable program code for encrypting the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

52. A system comprising:

a platform having a unique platform identifier (ID); and

a digital signature system coupled to the platform to authenticate data, the digital signature system comprising:

a first storage to store the platform identifier;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and

a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.

53. The system of claim 52 wherein the signature generator comprises:

a platform-specific transformer to transform the authentication identifier using the platform identifier to output an encrypted platform private key; and

a decryptor coupled to the platform-specific transformer to decrypt the encrypted platform private key to generate the platform private key using an authentication public key, the authentication public key being provided by the authentication vendor.

54. The system of claim 53 wherein the signature generator further comprises:

a signer coupled to the decryptor to sign the data using the platform private key, the platform private key being transparent to the platform.

55. The system of claim 53 wherein the platform-specific transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the platform identifier and the authentication identifier.

56. The system of claim 53 wherein the platform-specific transformer comprises:

a decryptor to decrypt the authentication identifier using a symmetric encryption/decryption key generated from the platform identifier.

57. The system of claim 53 wherein the authentication identifier is generated by a platform-specific reverse transformer which transforms the encrypted platform private key and the platform identifier, the encrypted platform private key being encrypted from the platform private key using the authentication private key.

58. The system of claim 57 wherein the platform-specific reverse transformer comprises an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier.

59. The system of claim 55 wherein the platform identifier is a unique, serially uncorrelated bit stream.

60. The system of claim 57 wherein the platform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated from the platform identifier.

61. The system of claim 52 wherein the platform identifier is installed in the first storage in a protected environment.

62. The system of claim 61 wherein the protected environment is a system management basic input/output system table.

63. The system of claim 55 wherein the platform-specific transformer further comprises:

a reporting device to report the platform identifier to generate a tracked platform identifier.

64. The system of claim 52 wherein the platform identifier is a processor serial number retrieved from a processor.

65. A system comprising:

a digital signature system;

an authentication identifier generator coupled to the digital signature system, the authentication identifier generator comprising:

an encryptor to encrypt a platform private key using an authentication private key to generate an encrypted platform private key, the platform private key being provided by a platform; and a platform-specific reverse transformer to transform the encrypted platform private key to generate an authentication identifier using a platform identifier unique to the platform, the authentication identifier being provided to the platform to generate a digital signature.

66. The system of claim 65 wherein the platform-specific reverse transformer comprises:

an Exclusive OR (XOR) device to perform an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

67. The system of claim 66 wherein the platform identifier is a unique, serially uncorrelated bit stream.

68. The of system claim 65 wherein the transform-specific reverse transformer comprises an encryptor to encrypt the encrypted platform private key using a symmetric encryption/decryption key generated by the platform identifier.

a first storage to store a platform identifier unique to a platform;

a second storage to store an authentication identifier, the authentication identifier being provided by an authentication vendor using the platform identifier, a platform private key, and an authentication private key; and a signature generator to generate a digital signature for data using the platform identifier and the authentication identifier.